(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-301831
(P2006-301831A)
(43)公開日　平成18年11月2日(2006.11.2)

(51) Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B285
G09C 1/00	(2006.01)	G09C	1/00	640E	5J104

審査請求 未請求　請求項の数 7　ＯＬ　（全 18 頁）

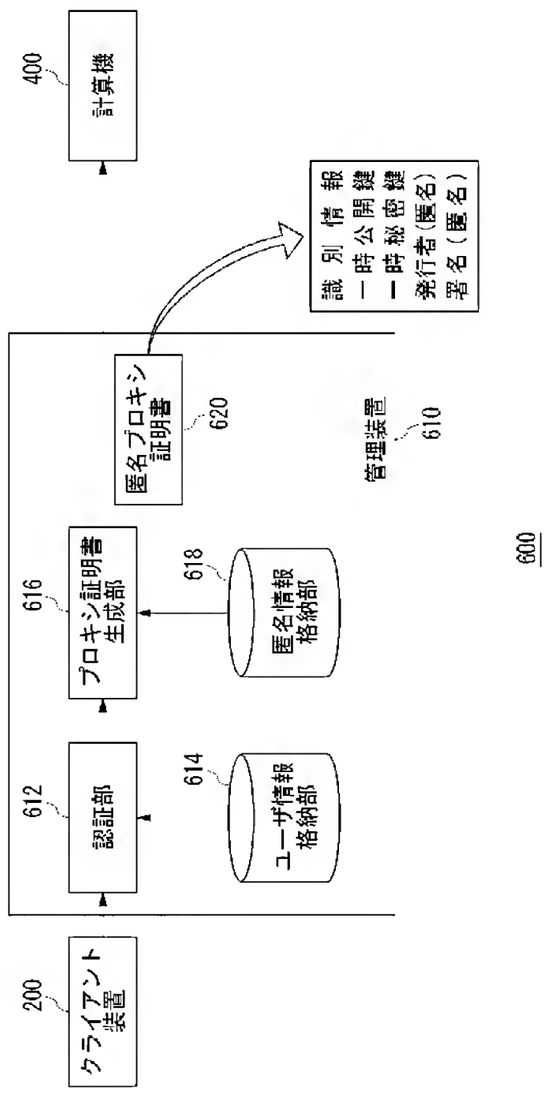
(21)出願番号　特願2005-120627 (P2005-120627)
(22)出願日　平成17年4月19日 (2005.4.19)

(71)出願人　301021533
独立行政法人産業技術総合研究所
東京都千代田区霞が関１－３－１
(71)出願人　301063496
東芝ソリューション株式会社
東京都港区芝浦一丁目１番１号
(74)代理人　100105924
弁理士　森下　賢樹
(72)発明者　田中　良夫
茨城県つくば市東１－１－１　独立行政法人産業技術総合研究所つくばセンター内
(72)発明者　関口　智嗣
茨城県つくば市東１－１－１　独立行政法人産業技術総合研究所つくばセンター内

最終頁に続く

(54)【発明の名称】管理装置

(57)【要約】
【課題】グリッド環境において利用される委譲手続きにより、ユーザの個人情報が計算機に伝達されてしまう。
【解決手段】グリッドシステム６００は、ＳＳＬでクライアント装置２００と接続し、ユーザのＩＤやパスワードに基づいて認証を行う。認証に成功した場合、認証部６１２は匿名プロキシ証明書の生成をプロキシ証明書生成部６１６に指示する。プロキシ証明書生成部６１６は、予め登録されている匿名ユーザの情報を匿名情報格納部６１８から読み込み、その匿名情報に基づいて匿名プロキシ証明書６２０を生成する。管理装置６１０は、その匿名プロキシ証明書６２０を利用して、計算機４００に対して認証処理を行い、ジョブを実行させる。計算機４００は管理装置６１０を信用することにより、匿名プロキシ証明書６２０の正当性を受け入れる。このように匿名プロキシ証明書６２０を利用することにより、計算機４００にユーザの個人情報が伝達されることを防止できる。
【選択図】図２



【特許請求の範囲】
【請求項１】
ユーザを直接的に特定可能な第１ユーザ情報を利用して、グリッド環境の利用を許可すべきユーザであるか否かを判断する認証部と、
前記ユーザの認証に成功した場合、前記第１ユーザ情報とは無関係に予め用意された第２ユーザ情報に基づいて、前記グリッド環境において利用されるプロキシ証明書を生成する生成部と、
前記プロキシ証明書を利用して、前記グリッド環境における所定の処理を行う計算機に利用許可を要求する要求部と、
を備えることを特徴とする管理装置。
【請求項２】
複数のそれぞれ異なる前記第２ユーザ情報を保持する匿名ユーザ情報格納部を更に備え、前記生成部は前記匿名ユーザ情報格納部に保持されている第２ユーザ情報のいずれかひとつを利用して前記プロキシ証明書を生成することを特徴とする請求項１に記載の管理装置。
【請求項３】
前記認証部において認証に成功した第１ユーザ情報と、プロキシ証明書の生成に利用した第２ユーザ情報とを対応付けるマッピング処理部と、
マッピングした第１ユーザ情報と第２ユーザ情報とを対応付けて保持するマッピングテーブルと、
所定の第２ユーザ情報に対応付けられて前記計算機から提供された前記所定の処理の実行結果を受け付ける処理結果受付部と、
前記マッピングテーブルを参照して、前記実行結果に対応付けられた前記所定の第２ユーザ情報に対応する第１ユーザ情報を特定し、その第１ユーザ情報で特定されるユーザに前記実行結果を提供するジョブ管理部と、
を更に備えることを特徴とする請求項１または２に記載の管理装置。
【請求項４】
第２ユーザ情報に対応付けられた第１ユーザ情報で特定される所定のユーザに関係する情報の提供要求を前記計算機から受け付け、その提供要求に応じて、前記所定のユーザに関係する属性情報を前記計算機に送信する応答部を更に備えることを特徴とする請求項１から３のいずれかに記載の管理装置。
【請求項５】
前記計算機に提供可能な前記属性情報のリストを保持する属性リスト格納部を更に備え、
前記応答部は、前記計算機に要求された場合に、前記リストの情報を送信することを特徴とする請求項４に記載の管理装置。
【請求項６】
前記応答部は、前記所定のユーザに関係する詳細なユーザ情報を一般化して生成された前記属性情報を前記計算機に送信することを特徴とする請求項４または５に記載の管理装置。
【請求項７】
前記実行結果を所定の第２ユーザ情報に対応付けて格納する結果格納部と、
前記計算機から所定の第２ユーザ情報に対応付けられた実行結果を要求された場合、前記結果格納部に保持されている前記所定の第２ユーザ情報に対応付けられた前記実行結果をその計算機に提供するファイル管理部と、
を更に備えることを特徴とする請求項３から６のいずれかに記載の管理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明はグリッドコンピューティング技術に関し、とくにグリッド環境において認証

を行う装置およびシステムに関する。

【背景技術】

【０００２】

ネットワーク技術が発達することにより、例えば電子メールが日常的に利用され、また様々なウェブサイトが多種多様なサービスを提供し、利用されている。このようなネットワークの利用は、今や当然の情報取得手段として我々の日々の生活に浸透しつつある。ネットワーク技術の発達にともない、様々な機器がネットワークに接続されるようになった。こうした中、グリッドコンピューティングと呼ばれる計算機の利用形態が生まれた。グリッドコンピューティングは、ネットワークを介して複数のコンピュータ資源を接続することにより、高性能なコンピュータを仮想的に形成し、ユーザが必要とする処理能力を提供することができる。グリッドコンピューティングを実現するシステムを、以下、「グリッドシステム」という。また、グリッドシステムが提供し、ユーザが享受するサービス環境を「グリッド環境」という。

【０００３】

図１（ａ）は、従来のグリッドシステム１０の構成図である。第１計算機２０ａ、第２計算機２０ｂ、および第３計算機２０ｃ（以下、単に「計算機２０」という）は、例えば所定の企業や研究所のコンピュータであり、グリッドシステム１０におけるコンピュータ資源として利用される。一般にそれぞれの計算機２０は、独立して機能し、独自のユーザ認証システムを有する。このため、ユーザは、利用する計算機２０毎に認証作業を行う必要がある。この認証処理は、ＰＫＩ（Public Key Infrastructure）に基づいており、認証局１４が発行したユーザ証明書を利用して行われる。この認証処理の過程で、グリッドシステム１０はユーザにパスフレーズの入力を要求する。パスフレーズは、暗号化されたユーザの秘密鍵を復号するために利用され、その役割の重要さからビット数が長くなっている。そもそも、グリッドシステムは、複数の計算機２０を同時に利用して、一台の計算機２０では得られない高速な処理を実現することをひとつの目的としており、ひとつのジョブを実行するために複数の計算機２０を利用することが多い。このため、ユーザは、利用する計算機２０毎に、認証処理のためにパスフレーズを入力する必要が生じてしまう。この認証処理は、ユーザに対してかなりの負担になる。そこで、グリッドシステムでは証明書の連鎖を用いている。すなわち、ユーザによって発行された証明書を持っているものはそのユーザの権限を持っており、自分自身の証明書を発行することができる。これをプロキシ証明書と呼び、ユーザ証明書の代わりとする。プロキシ証明書の有効期限を短くする代わりに、それを暗号化せずにファイルに保存するようにしているため、パスフレーズの再入力なしに計算機間でユーザの認証が可能である。

【０００４】

一方、ユーザにとって、グリッドシステムの利用には、グリッドシステムについての知識を必要とする。そこで、グリッドシステムについての十分な知識がなくてもグリッドシステムを容易に利用可能とする目的で管理装置３０が設けられている場合が多い。管理装置３０は、グリッドシステムにおける各計算機２０のポータルサイトとして機能するグリッドポータルであり、クライアント装置４０が生成したプロキシ証明書４４を利用して代理的にそれぞれの計算機２０に対して認証処理を行う。これにより、ユーザは利用する計算機２０毎に、自ら認証処理を行わなくて済む。また、管理装置３０は、ユーザからクライアント装置４０を介して指定された処理内容に応じて、処理に利用する計算機２０を選択し、選択した計算機２０に対して認証処理を行う。

【０００５】

クライアント装置４０は、ユーザが操作する端末装置であり、プロキシ証明書４４を発行し管理装置３０に提供するとともに、計算機２０に対する処理内容を管理装置３０に指示する。プロキシ証明書４４を発行し管理装置３０に提供する機能と、計算機２０に対する処理内容を管理装置３０に指示する機能とはそれぞれ異なる装置で提供されてもよいし、同一の装置で提供されてもよい。クライアント装置４０は、プロキシ証明書４４を生成するためのプロキシ証明書生成部４２を有する。グリッドシステム１０の利用にあたり、

最初に、ユーザは、プロキシ証明書生成部４２を利用して、プロキシ証明書４４を生成する。そして、クライアント装置４０と管理装置３０との間で委譲（delegation）が行われることにより、管理装置３０上にユーザのプロキシ証明書が生成される。その後、クライアント装置４０は、ウェブブラウザを利用して管理装置３０にアクセスし、サービス画面を表示する。管理装置３０は、クライアント装置４０からのプロキシ証明書４４を保持し、必要に応じて認証処理に利用することができる。

【０００６】

具体的には、プロキシ証明書生成部４２は、Globus toolkitにより実現され、管理装置３０は、Myproxy serverにより実現される。クライアント装置４０において、コマンド「grid-proxy-init」が実行されるとGlobus toolkitはプロキシ証明書４４を生成する。そして、コマンド「myproxy-init」が実行されると、管理装置３０は新しい公開鍵と秘密鍵のペアを作成し、その公開鍵をもとにＣＳＲ（Certificate Signing Request）を作成してクライアント装置４０に送信する。クライアント装置４０では予め生成しておいた一時秘密鍵（クライアント側で予め生成されているプロキシ証明書に格納されている公開鍵に対応する秘密鍵）でＣＳＲに署名をしたものと、予め作成しておいたプロキシ証明書のベースになるファイル７０を管理装置３０に送信する。管理装置３０はクライアントから送られてきたファイル７０に一時秘密鍵を添付することにより、管理装置３０にプロキシ証明書が作成される。そして、管理装置３０のMyproxy serverにプロキシ証明書４４が格納される。Myproxy serverはグリッドポータルである管理装置３０上で動作してもよいし、管理装置３０とは異なる装置上で動作してもよい。いずれの形態でも、Myproxy serverが動作する装置と管理装置３０との間で委譲が行われることにより、管理装置３０上にユーザのプロキシ証明書４４が生成される。

【０００７】

図１（ｂ）は、プロキシ証明書ファイル７０のデータ構造と生成処理を説明するための図である。図１（ａ）のプロキシ証明書生成部４２は、図１（ａ）の認証局１４が発行したユーザ証明書５０と、秘密鍵５２とに基づいて、プロキシ証明書ファイル７０を発行する。プロキシ証明書生成部４２は、一時的に利用する一時秘密鍵７４と一時公開鍵７６とを生成する。そして、プロキシ証明書生成部４２は、一時公開鍵７６をユーザ秘密鍵５２で署名、つまり暗号化する。このとき、暗号化されたユーザ秘密鍵５２を復号する必要があるので、ユーザは一度だけパスフレーズ５４を入力する。

【０００８】

プロキシ証明書４４は、一時公開鍵７６をユーザ秘密鍵５２で署名したものであり、プロキシ証明書４４にユーザ証明書５０を添付することで、プロキシ証明書４４の正当性が保証され、かつユーザ証明書５０の正当性は図１（ａ）の認証局１４により保証される。そして、このように保証された一時公開鍵７６に対応する一時秘密鍵７４も正当性が保証される。

【０００９】

ここで、一時秘密鍵７４は、ユーザ秘密鍵５２のようにパスフレーズ５４で暗号化されていない。これにより、管理装置３０は、ユーザからパスフレーズ５４を受け付けることなく、計算機２０に対する認証処理が可能になる。プロキシ証明書ファイル７０は、プロキシ証明書４４、一時秘密鍵７４、およびユーザ証明書５０を含む。図１（ａ）のクライアント装置４０と管理装置３０との間では委譲を行うことにより、管理装置３０上にユーザのプロキシ証明書が生成される（非特許文献１）。

【非特許文献１】「ハイパフォーマンスコンピューティングシステム」、情報処理学会論文誌Ｖｏｌ．４３、Ｎｏ．ＳＩＧ６（ＨＰＳ５）、ｐ１７２－ｐ１８３、２００２年

【発明の開示】

【発明が解決しようとする課題】

【００１０】

図１（ａ）のプロキシ証明書生成部４２は、所定のプログラムを実行することによりクライアント装置４０に形成される。そのため、ユーザはそのプログラムをクライアント装

置４０に予めインストールする必要がある。また、グリッドシステム１０を利用する前に、プロキシ証明書ファイル７０を生成するためのコマンドを実行し、その後、プロキシ証明書ファイル７０を管理装置３０に送信するためのコマンドを実行する必要がある。これらの作業は、コマンドプロンプトを利用して行われる。

【００１１】

グリッドコンピューティングは、ＵＮＩＸ（登録商標）やＬＩＮＵＸなどのＯＳを利用して、各種の研究や開発を行う研究者や技術者により利用されてきた。このため、グリッド環境は、例えばコマンドプロンプトを利用してコマンドを実行するという作業に慣れたユーザに多く利用されており、一般ユーザの利用という観点からの考察が十分に行われていなかった。

【００１２】

本発明者は、例えば電子メールが日常的に利用されている様に、今後グリッド環境が日常的に利用されることを考えた場合、コマンドプロンプトを利用する形態では一般ユーザに負担をかけるとともに、一般ユーザへの普及も望めないと考えた。更に、本発明者は、グリッドコンピューティングが普及し、例えば企業などが新しい商品の研究や、コンピュータグラフィックなど、非常に重要で極秘に取り扱われるべき情報を扱うことを考慮し、セキュアなグリッド環境を提供する必要があると考え、本発明に想到した。

本発明は上記課題に鑑みてなされたものであり、その目的は、グリッド環境における認証処理を容易にする技術、セキュアなグリッド環境を実現する技術を提供することにある。

【課題を解決するための手段】

【００１３】

本発明のある態様は、グリッド・コンピューティングシステムにおけるポータルサイトとして機能する管理装置に関する。この装置は、ユーザを直接的に特定可能な第１ユーザ情報を利用して、グリッド環境の利用を許可すべきユーザであるか否かを判断する認証部と、ユーザの認証に成功した場合、第１ユーザ情報とは無関係に予め用意された第２ユーザ情報に基づいて、グリッド環境において利用されるプロキシ証明書を生成する生成部と、プロキシ証明書を利用して、グリッド環境における所定の処理を行う計算機に利用許可を要求する要求部とを備える。計算機は、第１ユーザ情報とは無関係の第２ユーザ情報に基づいて生成されたプロキシ証明書に基づいて認証を行うので、ユーザの個人情報が計算機に伝達されることを防止でき、計算機に対して匿名性を確保できる。

【００１４】

この装置は、複数のそれぞれ異なる第２ユーザ情報を保持する匿名ユーザ情報格納部を更に備え、生成部は匿名ユーザ情報格納部に保持されている第２ユーザ情報のいずれかひとつを利用してプロキシ証明書を生成してもよい。これにより、それぞれ異なる匿名ユーザに署名されたプロキシ証明書をユーザ毎に生成することができる。

【００１５】

この装置は、認証部において認証に成功した第１ユーザ情報と、そのユーザのプロキシ証明書の生成に利用した第２ユーザ情報とを対応付けるマッピング処理部と、マッピングした第１ユーザ情報と第２ユーザ情報とを対応付けて保持するマッピングテーブルと、所定の第２ユーザ情報に対応付けられて計算機から提供された所定の処理の実行結果を受け付ける処理結果受付部と、マッピングテーブルを参照して、実行結果に対応付けられた所定の第２ユーザ情報に対応する第１ユーザ情報を特定し、その第１ユーザ情報で特定されるユーザに実行結果を提供するジョブ管理部とを更に備えてもよい。これにより、第２ユーザ情報に対応付けられた実行結果を、本来の依頼元であるユーザに提供することができる。

【００１６】

この装置は、第２ユーザ情報に対応付けられた第１ユーザ情報で特定される所定のユーザに関係する情報の提供要求を計算機から受け付け、その提供要求に応じて、所定のユーザに関係する属性情報を計算機に送信する応答部を更に備えてもよい。これにより、匿名

性を確保するとともに、ユーザの属性に応じたサービスを提供可能になる。
【００１７】
この装置は、計算機に提供可能な属性情報のリストを保持する属性リスト格納部を更に備えてよく、応答部は、計算機に要求された場合に、そのリストの項目を送信してもよい。これにより、提供可能な属性情報を計算機に予め通知できる。
【００１８】
応答部は、所定のユーザに関係する詳細なユーザ情報を一般化して生成された属性情報を計算機に送信してもよい。一般化することにより、属性情報に基づいて、ユーザを類推することを困難にできる。
【００１９】
この装置は、実行結果を所定の第２ユーザ情報に対応付けて格納する結果格納部と、計算機から所定の第２ユーザ情報に対応付けられた実行結果を要求された場合、結果格納部に保持されている所定の第２ユーザ情報に対応付けられた実行結果をその計算機に提供するファイル管理部とを更に備えてもよい。これにより、グリッド環境における複数の計算機を利用してジョブを処理する場合に、匿名性を確保したまま所定の計算機による計算結果を他の計算機が再利用することができる。
【００２０】
なお、以上の構成要素の任意の組合せ、本発明の表現を方法、装置、システム、記録媒体、コンピュータプログラムなどの間で変換したものもまた、本発明の態様として有効である。
【発明の効果】
【００２１】
本発明によれば、グリッド環境における認証処理を容易にすることができ、利便的でセキュアな認証処理を実現する装置およびシステムを提供できる。
【発明を実施するための最良の形態】
【００２２】
＜第１の実施の形態＞
図２は、第１の実施の形態に係るグリッドシステム６００の構成図である。各構成要素は、ハードウエアコンポーネントで言えば、任意のコンピュータのＣＰＵ、メモリ、メモリにロードされた本図の構成要素を実現するプログラム、そのプログラムを格納するハードディスクなどの記憶ユニット、ネットワーク接続用インターフェース等を中心に実現されるが、その実現方法、装置にはいろいろな変形例があることは、当業者には理解されるところである。これから説明する各図は、ハードウエア単位の構成ではなく、機能単位のブロックを示している。
【００２３】
クライアント装置２００は、ユーザが操作する端末装置であり、ネットワークを介して管理装置６１０に接続している。管理装置６１０は、クライアント装置２００を操作するユーザを認証する。そして、認証に成功した場合、そのユーザに依頼された処理を計算機４００に実行させる。計算機４００は、ネットワークを介して管理装置６１０と接続しており、管理装置６１０を認証する。そして、認証に成功した場合、計算機４００は、管理装置６１０から指示された処理を実行する。
【００２４】
管理装置６１０は、認証部６１２、ユーザ情報格納部６１４、プロキシ証明書生成部６１６、および匿名情報格納部６１８を有する。ユーザ情報格納部６１４は、例えば、ユーザを識別する情報（以下、単に「実ユーザＩＤ」という）およびパスワードの組合せなど、グリッドシステム６００の利用を許可すべきユーザを認証するための、ユーザに直接関係する情報（以下、単に「実認証情報」という）を保持する。認証部６１２は、ユーザ情報格納部６１４に保持されている実認証情報に基づいて、クライアント装置２００を操作するユーザの認証を行う。認証部６１２は、例えばＳＳＬ（Secure Socket Layer）でクライアント装置２００と接続し、ユーザから実ユーザＩＤとパスワードを受け付けて認証

を行ってもよいし、ユーザから所定の認証局が発行したユーザ証明書を受け付けて、そのユーザ証明書に基づいて認証を行ってもよい。つまり認証部６１２は、クライアント装置２００を操作するユーザを直接的に特定可能な情報を用いて認証を行う。そして、認証に成功した場合、認証部６１２はプロキシ証明書の発行をプロキシ証明書生成部６１６に指示する。

【００２５】

匿名情報格納部６１８は、管理装置６１０が管理する計算機４００を利用するための識別情報を保持する。この識別情報は、クライアント装置２００のユーザとは無関係に、計算機４００に予め登録された情報である。つまり、この識別情報は、管理装置６１０の管理者と計算機４００の管理者との間で結ばれた契約に基づいて登録されたものであり、実際のユーザ情報の代わりに利用する実際のユーザとは無関係の情報（以下、単に「匿名情報」という）である。匿名情報は、匿名ユーザ名、公開鍵、秘密鍵、認証局による証明書（以下、単に「匿名証明書」という）などを含む。また、匿名情報格納部６１８は、単一の匿名情報だけを保持してもよいし、複数の異なる匿名情報を保持してもよい。

【００２６】

プロキシ証明書の発行を指示された場合、プロキシ証明書生成部６１６は、匿名情報格納部６１８に保持されている匿名情報を利用して、匿名プロキシ証明書６２０を生成する。この匿名プロキシ証明書６２０は、図１（ｂ）を用いて説明したプロキシ証明書と同一のデータ構造をしており、匿名情報格納部６１８に保持されている匿名情報で署名されている。管理装置６１０は、この匿名プロキシ証明書６２０を用いて、計算機４００に対する認証処理を行い、計算機４００に所定の処理を実行させる。

【００２７】

このように、管理装置６１０がユーザに対しては実認証情報に基づいて認証を行い、計算機４００に対する指示は匿名情報を利用して行うことで、管理装置６１０はユーザに依頼された処理を計算機４００に匿名で実行させることができる。これにより、処理内容の依頼者つまりユーザの秘匿性を保つことができ、ユーザの個人情報がネットワークに流れることを最小限に抑えることができる。また、認証部６１２が、ユーザＩＤとパスワードによるベーシック認証を行うことにより、ユーザはクライアント装置２００にプロキシ証明書を生成するための専用プログラムを予めインストールし、毎回その専用プログラムを実行するといった作業が不要になる。これにより、グリッドシステム６００を利用するための認証処理を簡便にすることができる。

【００２８】

グリッド環境における処理の匿名性は、匿名情報格納部６１８がひとつの匿名情報を保持することで実現することができる。しかしながら、ユーザ毎に異なるサービスを提供したり、ユーザ毎に使用料金を設定したりすることは、ひとつの匿名情報だけでは困難である。そこで、以下に複数の匿名情報を利用することにより、匿名性を確保しつつ、ユーザ毎にサービスを提供可能にする形態を説明する。

【００２９】

＜第２の実施の形態＞

第２の実施の形態の要素技術は主に３つある。第１の技術は「複数の匿名情報を利用して、ユーザ毎に匿名プロキシ証明書を発行する技術」である。第２の技術は「ユーザ毎にサービス内容を変えてきめ細かなサービスを提供するために、匿名性を保ちながらユーザの属性を提供する技術」である。第３の技術は「匿名性を保ちながら過去の計算結果を使用する、もしくは他のユーザに公開するといったデータの再利用を可能にする技術」である。まず、これらの要素技術について説明する。

【００３０】

図３は、第１の要素技術である「複数の匿名情報を利用して、ユーザ毎に図２の匿名プロキシ証明書６２０を生成する技術」を説明するための図である。グリッドポータルサイトとして機能する管理装置１００は、匿名情報を複数保持し、それぞれのユーザ６３０に対応して、匿名プロキシ証明書６２０を生成する。その匿名プロキシ証明書６２０は、匿

名情報に含まれる匿名ユーザにより署名されている。そして、管理装置１００は各ユーザ６３０からの処理内容に基づいて、その処理に適した適当なサーバ６３２をグリッド環境の中から選択し、処理を指示する。サーバ６３２は、匿名プロキシ証明書６２０の発行者である匿名ユーザの匿名ユーザ証明書に基づいて、認証を行う。そして、認証に成功した場合、サーバ６３２はリソースを割り当て、プロセスを実行する。これにより、ユーザ６３０毎に匿名プロキシ証明書６２０を生成できるので、各ユーザ６３０と匿名ユーザとを一対一に対応付けて、グリッド環境における処理を管理することができる。

【００３１】

図４は、第２の要素技術である「匿名性を保ちながらユーザの属性を提供する技術」を説明するための図である。管理装置１００は、ユーザ６３０のユーザ属性証明書６３４を生成する。そして、管理装置１００は、そのユーザ属性証明書６３４をユーザ６３０に対応付けられた匿名ユーザの属性として匿名属性証明書６３６に変換する。この匿名属性証明書６３６は、例えば年齢、性別、会員情報の有無、職種、居住地などのユーザ属性証明書６３４に含まれる個人情報を一般化したデータを含み、グリッド環境におけるサービス内容に応じて任意に定義される。管理装置１００は、プロセスの実行要求に先立ち、サーバ６３２に実行条件を打診する（Ｓ１００）。サーバ６３２は、実行条件に基づいて、ユーザの属性を問い合わせる（Ｓ１０２）。そして、管理装置１００は、その問い合わせに応じたユーザの属性をサーバ６３２に回答する（Ｓ１０４）。これにより、管理装置１００は匿名性を保ちながら、ユーザの属性を提供することができる。この技術により、例えばサービス提供側すなわちサーバ６３２側がユーザの会員権や所属などの各種のユーザ属性に応じて、使用料金の割引や優先的に処理を行うことなど種々の特典を設定することができる。こうした特典により、サービス提供側は他との差別化を図ることができ、グリッド環境におけるビジネスに競争の原理を持ち込み、サービス提供者間の競争を激化し、グリッド環境そのものを活性化できる。

【００３２】

図５は、第３の要素技術である「匿名性を保ちながら過去の計算結果を使用する、もしくは他のユーザに公開するといったデータの再利用を可能にする技術」を説明するための図である。管理装置１００は、ユーザ６３０に対する処理を実名に基づいて処理する実名処理部１０２と、匿名で処理する匿名処理部１０４とを備える。実名処理部１０２は、実認証情報に基づいて、ユーザ６３０の認証を行い、認証に成功した場合、実ユーザと匿名ユーザとを対応付けてマッピングする。匿名処理部１０４は、実ユーザにマッピングされた匿名ユーザの情報を利用して、匿名ユーザとしてサーバ６３２に所定の処理を依頼する。

【００３３】

サーバ６３２は、前述した匿名プロキシ証明書６２０に基づいて、匿名ユーザの認証を行う。そして、認証に成功した場合、サーバ６３２は、所定の処理を実行し、計算の途中で生成されたテンポラリ・ファイルなどを一時的なデータとして格納し、計算結果を管理装置１００に提供する。そして、サーバ６３２は、例えば計算結果を管理装置１００に提供したことを契機に、計算結果やテンポラリ・ファイルを消去する。これにより、サーバ６３２からの計算結果等の漏洩を防止もしくは抑制できる。管理装置１００は、サーバ６３２から提供された計算結果を、匿名ユーザ名に基づいて短期間アクセス可能な短期保存データ９６と、実ユーザ名に基づいて長期間アクセス可能な長期保存データ９４とに分けて格納する。このように、管理装置１００が実ユーザ名と匿名ユーザ名とのマッピングを解決し、計算結果などのデータへのアクセス制御を行う。これにより、匿名性を保ちつつ、データの再利用を可能にできる。

【００３４】

これら３つの要素技術を、グリッド環境において提供するサービス内容に応じて、適切に組合せることにより、グリッド環境におけるシングル・サインオンを実現し、セキュアで利便性の高い利用環境をユーザに提供するポータルサイト、つまり管理装置１００を実現することができる。要素技術の組合せは任意であり、管理装置１００に全ての要素技術

が組み込まれてもよいし、一部の要素技術が組み込まれてもよい。

【００３５】

図６は、第２の実施の形態に係るグリッドシステム５００の構成図である。クライアント装置２００は、ユーザが操作する端末装置であり、ネットワークを介して管理装置１００に接続している。処理要求部２０２は、管理装置１００に対してグリッド環境を利用した処理を要求する。こうした処理を以下、単に「ジョブ」という。データ格納部２０４は、ジョブの実行に必要な、例えば変数、物質、関数、汎用データベースの名称などを保持する。データ格納部２０４に保持されるデータは、グリッド環境において実行する処理の内容により異なる。処理要求部２０２は、データ格納部２０４に保持されているデータとともに、ジョブの実行を管理装置１００に要求する。他の例では、処理要求部２０２は、直接ユーザからジョブの実行に必要なデータの入力を受け付けてもよい。また、処理要求部２０２は、ジョブの要求に先立ち、グリッド環境の利用の許否を実認証情報に基づいて行う。処理要求部２０２は、実際のユーザ情報を利用して管理装置１００に対する種々の指示を行う。

【００３６】

一方、結果受付部２０６は、管理装置１００からジョブを実行して得られた計算結果を受け付け、結果格納部２０８に格納する。表示処理部２１０は、結果格納部２０８に格納されている計算結果に基づいて、表示処理を行う。こうした、クライアント装置２００における一連の処理は、例えば専用のネットワーククライアントで実現されてもよいし、ウェブブラウザなどの汎用的なネットワーククライアントで実現されてもよい。好ましくは、ウェブブラウザで実現される形態である。

【００３７】

管理装置１００は、クライアント装置２００を操作するユーザを、実認証情報に基づいて認証し、匿名ユーザからの依頼としてアプリケーション提供装置３００にジョブを依頼する。管理装置１００は、主にユーザの実名に基づいて、認証処理や属性情報に関する処理を行う実名処理部１０２、ユーザの情報を匿名に変えて、匿名にてアプリケーション提供装置３００に対して認証処理を行う匿名処理部１０４、および匿名でジョブの実行を指示し、その計算結果を管理するジョブ管理部１１０を有する。匿名情報生成部１０６は、図３を用いて説明した第１の要素技術を実現するブロックであり、アプリケーション提供装置３００および計算機４００に対して処理を指示するための匿名情報すなわち匿名プロキシ証明書を生成する。

【００３８】

属性情報管理部１０８は、図４を用いて説明した第２の要素技術を実現するブロックであり、匿名の属性情報を管理する。属性情報管理部１０８は、アプリケーション提供装置３００との間で、ユーザの所属や権利などに応じた使用料金などの、アプリケーション提供装置３００および計算機４００の利用に関わる条件交渉を、匿名属性情報を用いて行う。これにより、属性情報管理部１０８は匿名にて、ユーザの属性に応じた条件交渉を行うことができる。

【００３９】

ジョブ管理部１１０はアプリケーション提供装置３００から計算結果を受け付け、それを管理装置１００の一時格納部１１２に格納するとともに、クライアント装置２００と接続して計算結果を提供する。管理装置１００の削除部１１４は、計算結果をクライアント装置２００に提供したことを検出すると、一時格納部１１２に保持されている計算結果を削除する。他の例で、削除部１１４は、計算結果の提供前であっても、所定の時間が経過した場合、一時格納部１１２から計算結果を削除してもよい。このように、管理装置１００は、クライアント装置２００とは、ユーザの実名に基づいて通信を行い、アプリケーション提供装置３００とは匿名すなわち間接的なユーザの情報に基づいて通信を行う。これにより、アプリケーション提供装置３００に対しては、ユーザの個人情報を隠蔽することができる。

【００４０】

アプリケーション提供装置３００は、複数の計算機４００を配下に有し、例えばジョブの内容や各計算機４００におけるジョブの実行状態すなわち計算機４００の稼働状態に応じて、ジョブを振り分ける。そして、アプリケーション提供装置３００は、計算結果を計算機４００から受け付け、管理装置１００に中継する。

【００４１】

匿名認証部３０２は、管理装置１００がユーザの実名の代わりに利用する匿名ユーザの認証を行う。指示部３０４は、ジョブの内容を受け付け、そのジョブを実行するためのプログラムをアプリケーション格納部３０６から読み込む。そして、指示部３０４は、そのプログラムとともに、ジョブの実行を計算機４００に指示する。アプリケーション提供装置３００が計算機４００にジョブの実行を指示する前段に、匿名プロキシ証明書を利用して委譲による認証が行われる。匿名プロキシ証明書には、ユーザに関する情報が含まれていないため、委譲された企ての計算機にユーザの個人情報が渡されることはない。

【００４２】

中継部３０８は、計算結果を計算機４００から受け付け、アプリケーション提供装置３００の一時格納部３１２に格納する。そして、中継部３０８は、計算結果を管理装置１００に提供する。つまり、中継部３０８は、計算機４００がジョブを実行することにより算出した計算結果を管理装置１００に中継する。削除部３１０は、計算結果の提供が完了したことを契機として、一時格納部３１２に一時的に格納されている計算結果を削除する。このように、計算結果を積極的に削除することにより、アプリケーション提供装置３００を介して計算結果が漏洩することを防止できる。

【００４３】

計算機４００は、ジョブを実際に処理し、計算結果をアプリケーション提供装置３００に提供する。また、計算機４００は、必要に応じて汎用データ提供装置２５０に保持されている汎用データを利用して、ジョブを処理する。汎用データ提供装置２５０は、汎用データを汎用データ格納部２５２に保持しており、例えば遺伝子情報、物性情報、気象情報など各種のデータを保持するデータベースであってよい。

【００４４】

処理要求受付部４０２は、アプリケーション提供装置３００から匿名にてジョブを受け付け、ジョブを実行するためのプログラムを実行部４０４に供給する。この処理の前段として、アプリケーション提供装置３００から委譲された匿名プロキシ証明書を受け付け、委譲による認証処理が行われる。取得部４０６は、そのプログラムが必要とする汎用データを汎用データ提供装置２５０から取得し、実行部４０４に供給する。実行部４０４は、プログラムを実行し、実行結果を計算結果として提供部４０８に出力する。提供部４０８は、計算結果を一時格納部４１０に格納するとともに、アプリケーション提供装置３００に提供する。計算機４００の削除部４１２は、計算結果の提供が完了したことを契機として、一時格納部４１０に一時的に格納されている計算結果を削除する。このように、計算結果を積極的に削除することにより、計算機４００を介して計算結果が漏洩することを防止できる。

【００４５】

図７は、図６の管理装置１００の内部構成図である。管理装置１００は、図６を用いて説明したとおり、実名処理部１０２と匿名処理部１０４とを有する。本図で、ラインＬの左側が実名処理部１０２に該当し、右側が匿名処理部１０４に該当する。ユーザ情報管理部１３６は、ユーザの実認証情報や性別、年齢、所属などのユーザ属性を新たに受け付けユーザ情報格納部１３８に登録し、更新や削除を行う。ユーザ情報格納部１３８は、例えば実ユーザＩＤに対応付けて実認証情報やユーザ属性を保持する。認証部１２０は、クライアント装置２００からユーザＩＤやパスワードを受け付け、ユーザの認証をユーザ情報格納部１３８に保持されているデータを参照して行う。実名による認証に成功した場合、認証部１２０はその旨を匿名情報生成部１０６に通知する。もちろん、認証部１２０は、認証局が発行したユーザ証明書に基づいて、認証処理を行ってもよい。要は、認証部１２０は、ユーザを直接的に特定可能な情報を利用して、ユーザの認証を行えばよい。

【００４６】
匿名情報生成部１０６は、匿名ＩＤ管理部１２２、匿名プロキシ証明書生成部１２３、匿名プロキシ証明書格納部１２４、認証要求部１２８、および匿名ＩＤテーブル１２６を有する。匿名ＩＤテーブル１２６は、複数の匿名ユーザの情報、すなわち匿名情報を保持する。匿名ＩＤテーブル１２６におけるデータ構造は任意であるが、匿名情報に加えて識別情報（以下、単に「匿名ＩＤ」という）と、その匿名情報を使用中であるかを示す使用フラグとを含む。

【００４７】
実名による認証が成功したことを認証部１２０から受け付けると、匿名ＩＤ管理部１２２は、匿名ＩＤテーブル１２６の利用フラグを参照して、未使用の匿名情報を選択する。そして、匿名ＩＤ管理部１２２は、選択した匿名情報を匿名ＩＤテーブル１２６から読み込み、匿名プロキシ証明書生成部１２３に出力するとともに、匿名プロキシ証明書の生成を指示する。

【００４８】
匿名プロキシ証明書生成部１２３は、図２を用いて説明した匿名プロキシ証明書６２０を生成し、匿名プロキシ証明書格納部１２４に格納する。認証要求部１２８は、匿名プロキシ証明書を利用してアプリケーション提供装置３００に認証処理を要求する。アプリケーション提供装置３００への認証が成功した場合、認証要求部１２８は、その旨を処理内容受付部１５０に通知する。詳細は後述するが、その通知を受けて、処理内容受付部１５０は、クライアント装置２００からジョブを受け付ける。

【００４９】
また、匿名ＩＤ管理部１２２は、匿名プロキシ証明書生成部１２３に匿名プロキシ証明書の生成を指示する一方で、選択した匿名情報とユーザとを対応付けることを匿名情報管理部１３０に指示する。匿名情報管理部１３０は、実ユーザと匿名ユーザとをマッピングするマッピング処理部１３２と、マップファイルを保持するマッピングテーブル１３４とを有する。具体的には、マッピング処理部１３２は、匿名ＩＤ管理部１２２から匿名ＩＤを受け付け、実ユーザＩＤと匿名ＩＤとを対応付けてマップファイルとしてマッピングテーブル１３４に登録する。これにより、実際のユーザと匿名ユーザとが対応付けられるので、管理装置１００はクライアント装置２００に対しては実名で処理を行い、アプリケーション提供装置３００および計算機４００に対しては匿名で処理を行うことができる。つまり、管理装置１００は、実ユーザに対する処理と匿名ユーザに対する処理とを相互に変換可能である。

【００５０】
属性情報管理部１０８は、図４を用いて説明した匿名属性証明書６３６を生成し、例えばジョブが有効な期間に渡り、管理する。属性情報管理部１０８は、属性証明書発行部１４０、匿名属性証明書発行部１４２、匿名属性証明書格納部１４４、属性リストテーブル１４６、および属性応答部１４８を有する。属性証明書発行部１４０は、ユーザ情報格納部１３８に保持されているユーザ属性に基づいて、図４を用いて説明したユーザ属性証明書６３４を発行する。匿名属性証明書発行部１４２は、そのユーザ属性証明書６３４に基づいて使用中の匿名ＩＤ毎の匿名属性証明書６３６を発行して、匿名属性証明書格納部１４４に格納する。

【００５１】
具体的には、匿名属性証明書発行部１４２は、マッピングテーブル１３４に保持されているマップファイルを参照して、使用中の匿名ＩＤに対応付けられた実ユーザＩＤを特定する。そして、匿名属性証明書発行部１４２は、特定した実ユーザＩＤのユーザ属性証明書６３４の提供を属性証明書発行部１４０に要求する。その要求に応じて、属性証明書発行部１４０は、ユーザ情報格納部１３８を参照して、指定された実ユーザＩＤで特定されるユーザのユーザ属性に基づいて、ユーザ属性証明書６３４を発行する。匿名属性証明書発行部１４２は、こうして発行されたユーザ属性証明書６３４に基づいて、匿名ＩＤに対応付け、例えばユーザ属性証明書６３４に保持されている属性を、更に上位概念の属性に

変換し匿名属性証明書６３６を生成する。

【００５２】

属性応答部１４８は、アプリケーション提供装置３００からの要求に応じて、匿名属性証明書格納部１４４に保持されている匿名属性証明書６３６をアプリケーション提供装置３００に提供する。属性応答部１４８は、匿名属性証明書６３６全体をアプリケーション提供装置３００に提供してもよいし、匿名属性証明書６３６の一部を要求に応じて、その都度アプリケーション提供装置３００に提供してもよい。属性リストテーブル１４６は、アプリケーション提供装置３００に提供可能な属性のリストを保持する。そして、アプリケーション提供装置３００に属性リストの提供を要求された場合、属性応答部１４８は属性リストテーブル１４６から属性リストを読み込んで、アプリケーション提供装置３００に提供する。アプリケーション提供装置３００は、その属性リストに基づいて、ジョブの実行条件を満たすために必要な属性を属性応答部１４８に問い合わせてもよい。

【００５３】

また、匿名属性証明書格納部１４４は、属性毎に、提供に際してユーザの許可が必要か否かを指定する提供フラグを有する。属性応答部１４８は、その提供フラグにユーザの許可が必要であることを示すフラグが保持されている場合、その属性をアプリケーション提供装置３００に提供してよいか否かをクライアント装置２００に問い合わせる。また、提供フラグにユーザの許可は不要であることを示すフラグが保持されている場合、ユーザに問い合わせることなく自動的にその属性をアプリケーション提供装置３００に提供する。これにより、属性レベルの情報でさえも、ユーザの個人情報が管理装置１００の後段に存在するアプリケーション提供装置３００や計算機４００に必要以上に流出することを防止できる。

【００５４】

他の例では、属性応答部１４８は、匿名属性証明書格納部１４４に保持されている属性をそのままアプリケーション提供装置３００に送信するのではなく、アプリケーション提供装置３００からの「ユーザは××学会の会員ですか？」という問いに対して、「はい／いいえ」のどちらかで応答するような間接的な方法で属性を提供してもよい。具体的には、属性応答部１４８とアプリケーション提供装置３００との間で、応答のためのコマンドやＸＭＬ（eXtensible Markup Language）におけるタグなどを定義しておき、それらを利用して実行条件の交渉が行われる。つまり、属性応答部１４８は、匿名性を保ちつつ、匿名化されたユーザに関する情報を提供する機能を有すればよい。このような方法により、グリッドシステム５００は更に強固な匿名性を実現し、ユーザの個人情報の隠蔽を完全なものにできる。

【００５５】

前述の認証要求部１２８が、認証に成功した場合、処理内容受付部１５０は、ジョブをクライアント装置２００から受け付ける。例えば、処理内容受付部１５０は、ジョブを受け付けるための表示画面を形成するための例えばＨＴＭＬ（HyperText Markup Language）などの文書記述言語で構成された画面情報をクライアント装置２００に送信する。そして、処理内容受付部１５０は、その表示画面を介して入力されたジョブを、クライアント装置２００から受け付ける。処理内容受付部１５０は、受け付けたジョブを実ユーザＩＤに対応付けてスケジューリング処理部１５２に出力する。

【００５６】

スケジューリング処理部１５２は、ジョブをアプリケーション提供装置３００に要求する順序や時期などを、例えばその時のグリッド環境における計算機４００の稼働状態や、ユーザとの契約上の優先度などに基づいて計画する。そして、スケジューリング処理部１５２は、ジョブの実行計画を実ユーザＩＤに対応付けてジョブ管理部１１０に出力する。

【００５７】

ジョブ管理部１１０は、マッピングテーブル１３４を参照して、実ユーザＩＤに対応付けられた匿名ＩＤを特定し、特定した匿名ＩＤに対応付けてジョブを処理要求部１５４に出力する。処理要求部１５４は、匿名ＩＤとジョブとを対応付けてアプリケーション提供

装置３００に送信し、そのジョブの実行を要求する。この要求を受けて、アプリケーション提供装置３００は、前述した属性応答部１４８に対して実行条件の交渉のため、属性の問い合わせを行う。

【００５８】

処理結果受付部１５６は、アプリケーション提供装置３００から匿名ＩＤに対応付けられた計算結果を受け付け、ジョブ管理部１１０に供給する。ジョブ管理部１１０は、その計算結果を匿名ＩＤに対応付けてファイル管理部１５８に供給する。そして、ジョブ管理部１１０は、マッピングテーブル１３４を参照して匿名ＩＤに対応付けられた実ユーザＩＤを特定し、そのユーザのクライアント装置２００にジョブが完了したことを通知するメッセージを送信する。

【００５９】

ファイル管理部１５８は、計算結果を匿名ＩＤに対応付けて短期保存データ格納部１６２に格納し、実ユーザＩＤに対応付けて長期保存データ格納部１６０に格納する。ファイル管理部１５８は、短期保存データ格納部１６２に格納されている計算結果を所定の時間が経過した後、強制的に削除する。例えば、ファイル管理部１５８は、ジョブが完了したことを契機として、計算結果を削除してもよい。ここで、処理結果受付部１５６が受け付け、ジョブ管理部１１０がファイル管理部１５８に供給する計算結果は、ジョブに対する最終的な計算結果でもよいし、一連のジョブを実行する過程で、生成された途中の計算結果（以下、単に「テンポラリ・ファイル」という）でもよい。また、処理結果受付部１５６が受け付ける計算結果およびテンポラリ・ファイルを総称して、「受信ファイル」という。

【００６０】

処理結果受付部１５６が受け付ける受信ファイルには、テンポラリ・ファイルであるか、最終的な計算結果であるかを指定するファイル属性情報が対応付けられている。そして、ファイル管理部１５８は、ファイル属性情報に基づいて、受信ファイルを長期保存データ格納部１６０または短期保存データ格納部１６２に振り分けて格納する。図６の計算機４００の提供部４０８は、計算結果にファイル属性情報を対応付けてアプリケーション提供装置３００に提供する。これにより、処理結果受付部１５６は、ファイル属性情報の対応付けられた受信ファイルを受け付けることができる。

【００６１】

例えば、グリッド環境における複数の計算機４００を利用してジョブを行う場合、ファイル管理部１５８は、それぞれの計算機４００における計算結果を匿名ＩＤおよびジョブにおける変数名などに対応付けて短期保存データ格納部１６２に格納する。そして、その計算結果を利用する計算機４００から要求された場合、ファイル管理部１５８は、要求された計算結果を短期保存データ格納部１６２から読み込み、処理結果受付部１５６を介して計算機４００に提供する。本図では、管理装置１００と計算機４００とは直接通信は行わず、アプリケーション提供装置３００を介して行う形態を図示している。このように、短期保存データ格納部１６２は、一連のジョブを完了する際に生じる一時的な計算結果を格納するための一時格納エリアとして、グリッド環境における各計算機４００により利用される。これにより、匿名性を確保しつつ、計算機４００において生成された計算結果やテンポラリ・ファイルを再利用することが可能になる。

【００６２】

長期保存データ格納部１６０は、最終的に得られたジョブの計算結果を実ユーザＩＤに対応付けて保持する。これにより、ジョブ管理部１１０は、ユーザに要求された場合に、長期保存データ格納部１６０に保持されている計算結果をクライアント装置２００に提供することができる。

【００６３】

図８は、図６を用いて説明したグリッドシステム５００における各装置間の処理のシーケンスの一例を示す図である。本図で、アプリケーション提供装置３００および計算機４００は、まとめて記述している。以下、それらを単に計算機４００として説明する。まず

、クライアント装置２００は、実名でジョブの処理を要求する（Ｓ１０）。管理装置１００は、実認証情報に基づいてユーザの認証を行う（Ｓ１２）。認証に成功した場合、管理装置１００は、匿名プロキシ証明書を生成し（Ｓ１４）、計算機４００に認証処理を要求する（Ｓ１６）。

【００６４】

計算機４００は、匿名プロキシ証明書を利用して認証処理を行う（Ｓ１８）。認証に成功した場合、計算機４００は、ユーザの属性情報が必要か否かを判断する（Ｓ２０）。属性情報が必要な場合（Ｓ２０のＹ）、計算機４００は管理装置１００に属性情報を要求する（Ｓ２２）。管理装置１００は、図４を用いて説明した匿名属性証明書６３６を参照して、要求された属性情報を選択し（Ｓ２４）、計算機４００に送信する（Ｓ２６）。ここで、本実施の形態の管理装置１００は、ユーザに予め許可されている属性情報のみを、自動的に計算機４００に送信する。このため、計算機４００がユーザに許可されていない属性情報を要求した場合、必要な属性情報が得られていないことになる。このために次のステップ２８が設けられている。計算機４００は、必要な属性情報を全て取得できたか否かを判断する（Ｓ２８）。必要な属性情報が不足している場合（Ｓ２８のＮ）、計算機４００は実行条件を管理装置１００に通知する（Ｓ３０）。そして、管理装置１００は、その実行条件をクライアント装置２００に通知する（Ｓ３２）。

【００６５】

ユーザはその実行条件に応じて、属性情報の送信の許否を指定する情報を管理装置１００に送信する（Ｓ３４）。許可された場合（Ｓ３６のＹ）、管理装置１００はその属性情報を計算機４００に送信する（Ｓ４０）。また、拒否された場合（Ｓ３６のＮ）、管理装置１００は拒否されたことを示す情報を計算機４００に送信する（Ｓ３８）。そして、計算機４００は、再度、必要な属性情報を全て取得したか否かを判断する（Ｓ４２）。必要な情報を取得できなかった場合（Ｓ４２のＮ）、計算機４００はジョブを実行できないことを示すエラーメッセージを管理装置１００に送信する（Ｓ４４）。そして、管理装置１００は、そのエラーメッセージをクライアント装置２００に送信する（Ｓ４６）。

【００６６】

また、ステップ４２で、必要な情報を全て取得できた場合（Ｓ４２のＹ）、計算機４００は依頼されたジョブを実行し（Ｓ４８）、計算結果を管理装置１００に送信する（Ｓ５０）。そして、管理装置１００は、その計算結果をクライアント装置２００に送信する（Ｓ５２）。また、ステップ２０で、属性情報が必要無い場合（Ｓ２０のＮ）、計算機４００はジョブを実行する（Ｓ４８）。また、ステップ２８で、必要な情報を全て取得した場合（Ｓ２８のＹ）、計算機４００はジョブを実行する（Ｓ４８）。

【００６７】

以上、本発明を実施の形態をもとに説明した。この実施の形態は例示であり、それらの各構成要素や各処理プロセスの組合せにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【図面の簡単な説明】

【００６８】

【図１】図１（ａ）は、従来のグリッドシステムの構成図であり、図１（ｂ）は、プロキシ証明書ファイルのデータ構造と生成処理を説明するための図である。

【図２】第１の実施の形態に係るグリッドシステムの構成図である。

【図３】第１の要素技術である「複数の匿名情報を利用して、ユーザ毎に図２の匿名プロキシ証明書を生成する技術」を説明するための図である。

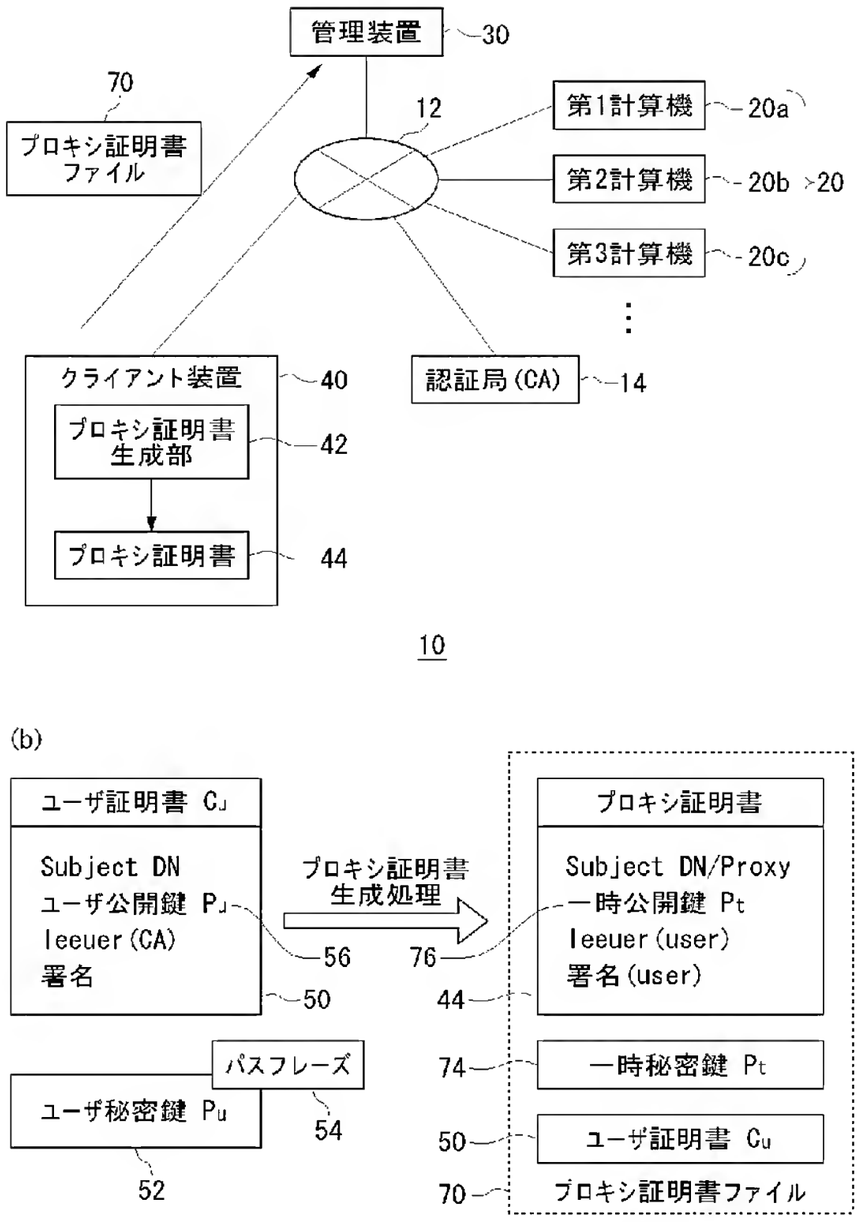
【図４】第２の要素技術である「匿名性を保ちながらユーザの属性を提供する技術」を説明するための図である。

【図５】第３の要素技術である「匿名性を保ちながら過去の計算結果を使用する、もしくは他のユーザに公開するといったデータの再利用を可能にする技術」を説明するための図である。

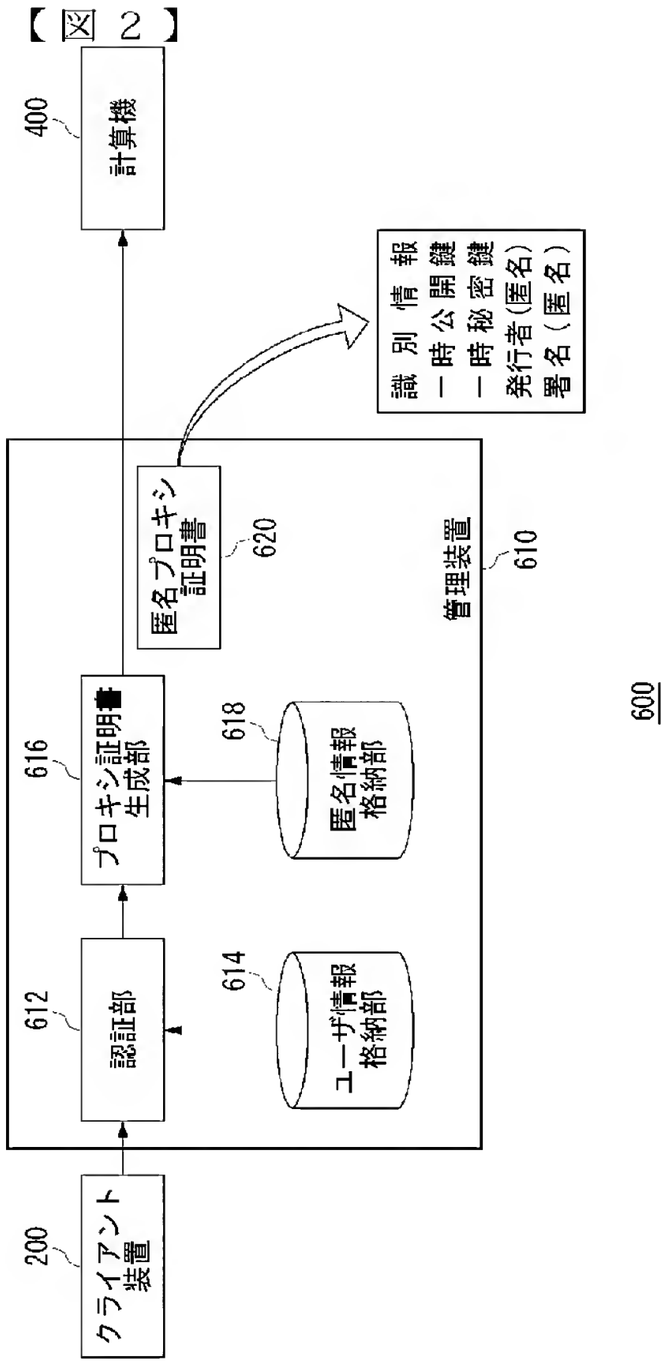
【図６】第２の実施の形態に係るグリッドシステムの構成図である。

【図７】図６の管理装置の内部構成図である。
【図８】図６を用いて説明したグリッドシステムにおける各装置間の処理のシーケンスの一例を示す図である。
【符号の説明】
【００６９】
１０　グリッドシステム、１２　ネットワーク、１４　認証局、２０　計算機、３０　管理装置、４０　クライアント装置、４２　プロキシ証明書生成部、４４　プロキシ証明書、５０　ユーザ証明書、５２　ユーザ秘密鍵、５４　パスフレーズ、５６　ユーザ公開鍵、７０　プロキシ証明書ファイル、７４　一時秘密鍵、７６　一時公開鍵、９４　長期保存データ、９６　短期保存データ、１００　管理装置、１０２　実名処理部、１０４　匿名処理部、１０６　匿名情報生成部、１０８　属性情報管理部、１１０　ジョブ管理部、１１２　一時格納部、１１４　削除部、１２０　認証部、１２２　匿名ＩＤ管理部、１２３　匿名プロキシ証明書生成部、１２４　匿名プロキシ証明書格納部、１２６　匿名ＩＤテーブル、１２８　認証要求部、１３０　匿名情報管理部、１３２　マッピング処理部、１３４　マッピングテーブル、１３６　ユーザ情報管理部、１３８　ユーザ情報格納部、１４０　属性証明書発行部、１４２　匿名属性証明書発行部、１４４　匿名属性証明書格納部、１４６　属性リストテーブル、１４８　属性応答部、１５０　処理内容受付部、１５２　スケジューリング処理部、１５４　処理要求部、１５６　処理結果受付部、１５８　ファイル管理部、１６０　長期保存データ格納部、１６２　短期保存データ格納部、２００　クライアント装置、２０２　処理要求部、２０４　データ格納部、２０６　結果受付部、２０８　結果格納部、２１０　表示処理部、２５０　汎用データ提供装置、２５２　汎用データ格納部、３００　アプリケーション提供装置、３０２　匿名認証部、３０４　指示部、３０６　アプリケーション格納部、３０８　中継部、３１０　削除部、３１２　一時格納部、４００　計算機、４０２　処理要求受付部、４０４　実行部、４０６　取得部、４０８　提供部、４１０　一時格納部、４１２　削除部、５００　グリッドシステム、６００　グリッドシステム、６１０　管理装置、６１２　認証部、６１４　ユーザ情報格納部、６１６　プロキシ証明書生成部、６１８　匿名情報格納部、６２０　匿名プロキシ証明書、６３０　ユーザ、６３２　サーバ、６３４　ユーザ属性証明書、６３６　匿名属性証明書。

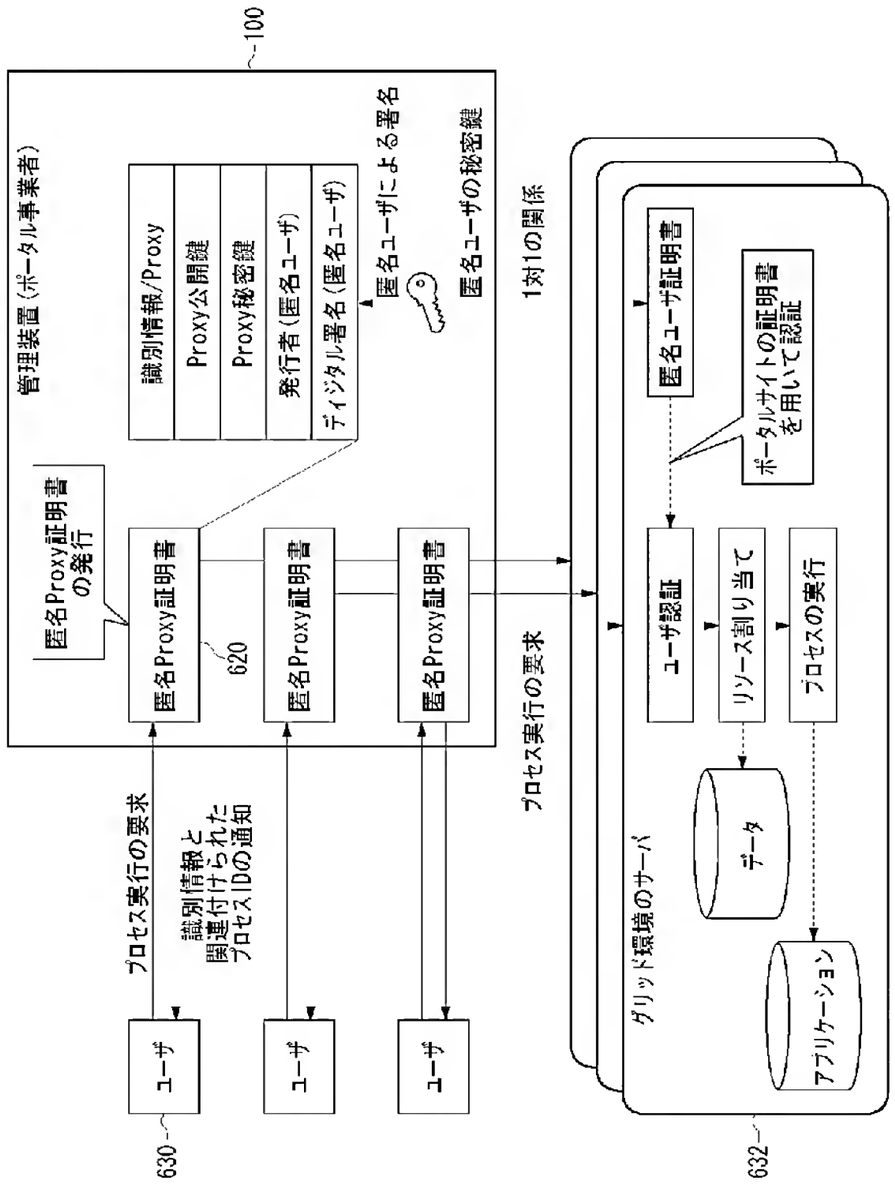
【図１】


(a)
管理装置
30
70
プロキシ証明書
ファイル
12
第1計算機
20a
第2計算機
20b
20
第3計算機
20c
クライアント装置
40
プロキシ証明書
生成部
42
プロキシ証明書
44
認証局(CA)
14
10
(b)
ユーザ証明書 Cu
Subject DN
ユーザ公開鍵 Pu
Ieeuer(CA)
署名
56
50
プロキシ証明書
生成処理
プロキシ証明書
Subject DN/Proxy
一時公開鍵 Pt
Ieeuer(user)
署名(user)
76
44
パスフレーズ
54
ユーザ秘密鍵 Pu
52
74
一時秘密鍵 Pt
50
ユーザ証明書 Cu
70
プロキシ証明書ファイル

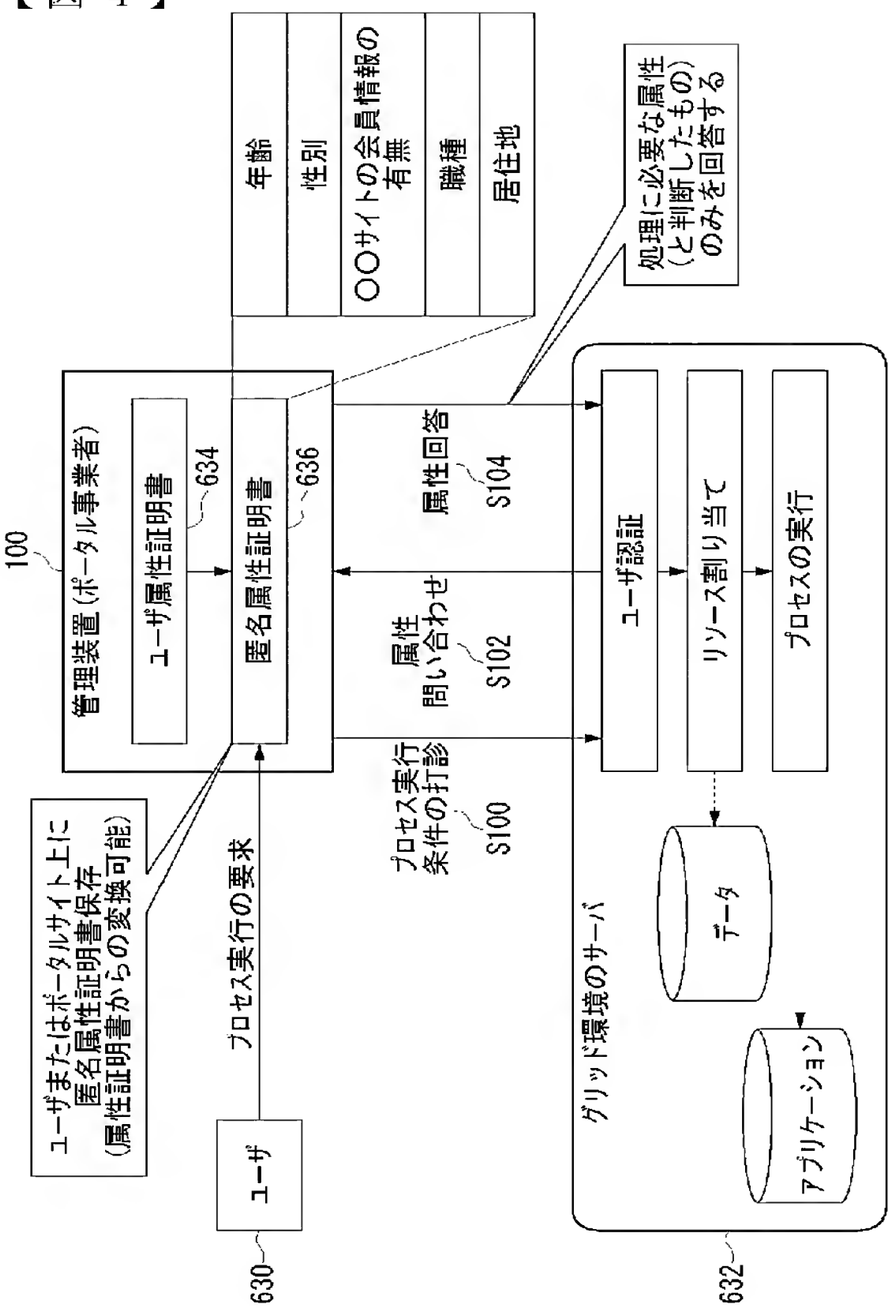
【図２】


400
計算機
識別情報
一時公開鍵
一時秘密鍵
発行者(匿名)
署名(匿名)
匿名プロキシ
証明書
620
管理装置
610
プロキシ証明書
生成部
616
618
匿名情報
格納部
認証部
612
614
ユーザ情報
格納部
600
クライアント
装置
200

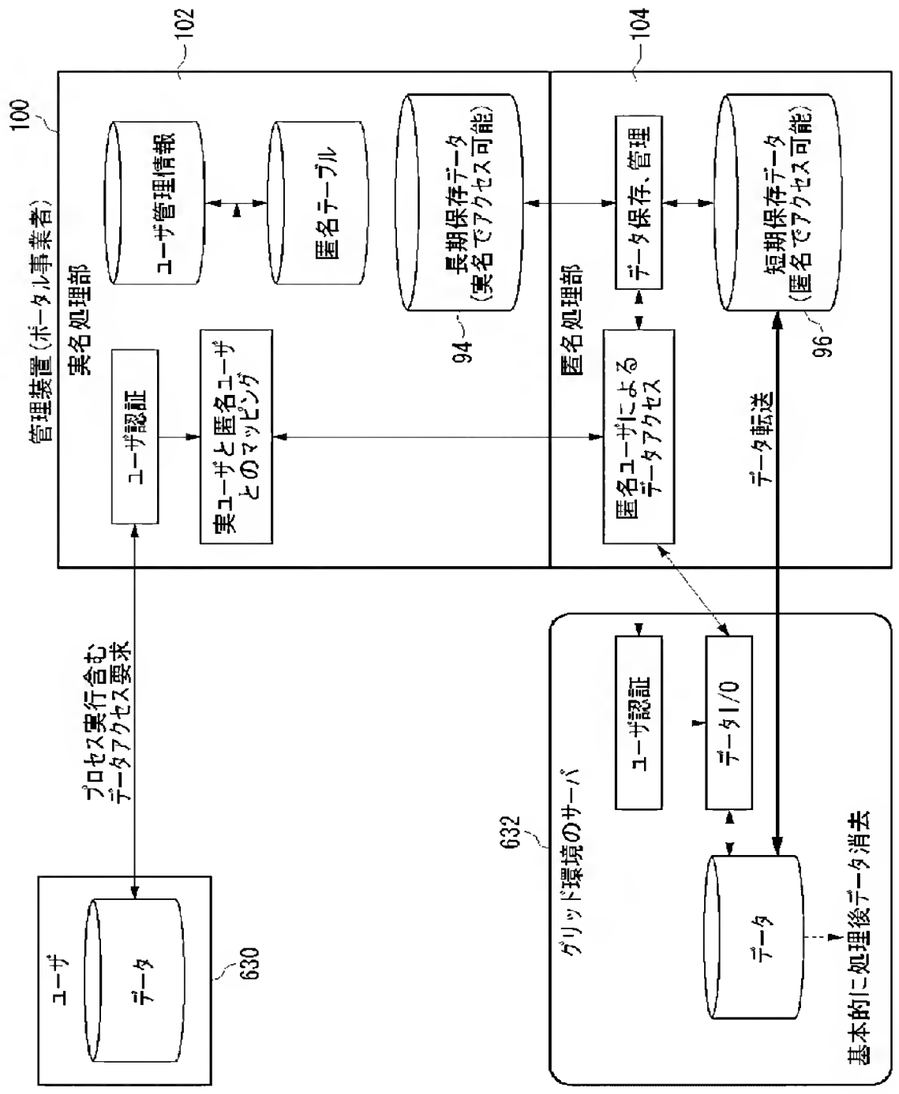
【図３】


100
管理装置(ポータル事業者)
識別情報/Proxy
Proxy公開鍵
Proxy秘密鍵
発行者(匿名ユーザ)
ディジタル署名(匿名ユーザ)
匿名ユーザによる署名
匿名ユーザの秘密鍵
匿名Proxy証明書の発行
匿名Proxy証明書
620
匿名Proxy証明書
匿名Proxy証明書
プロセス実行の要求
識別情報と
関連付けられた
プロセスIDの通知
ユーザ
ユーザ
ユーザ
630
1対1の関係
匿名ユーザ証明書
ポータルサイトの証明書
を用いて認証
プロセス実行の要求
グリッド環境のサーバ
ユーザ認証
リソース割り当て
プロセスの実行
データ
アプリケーション
632

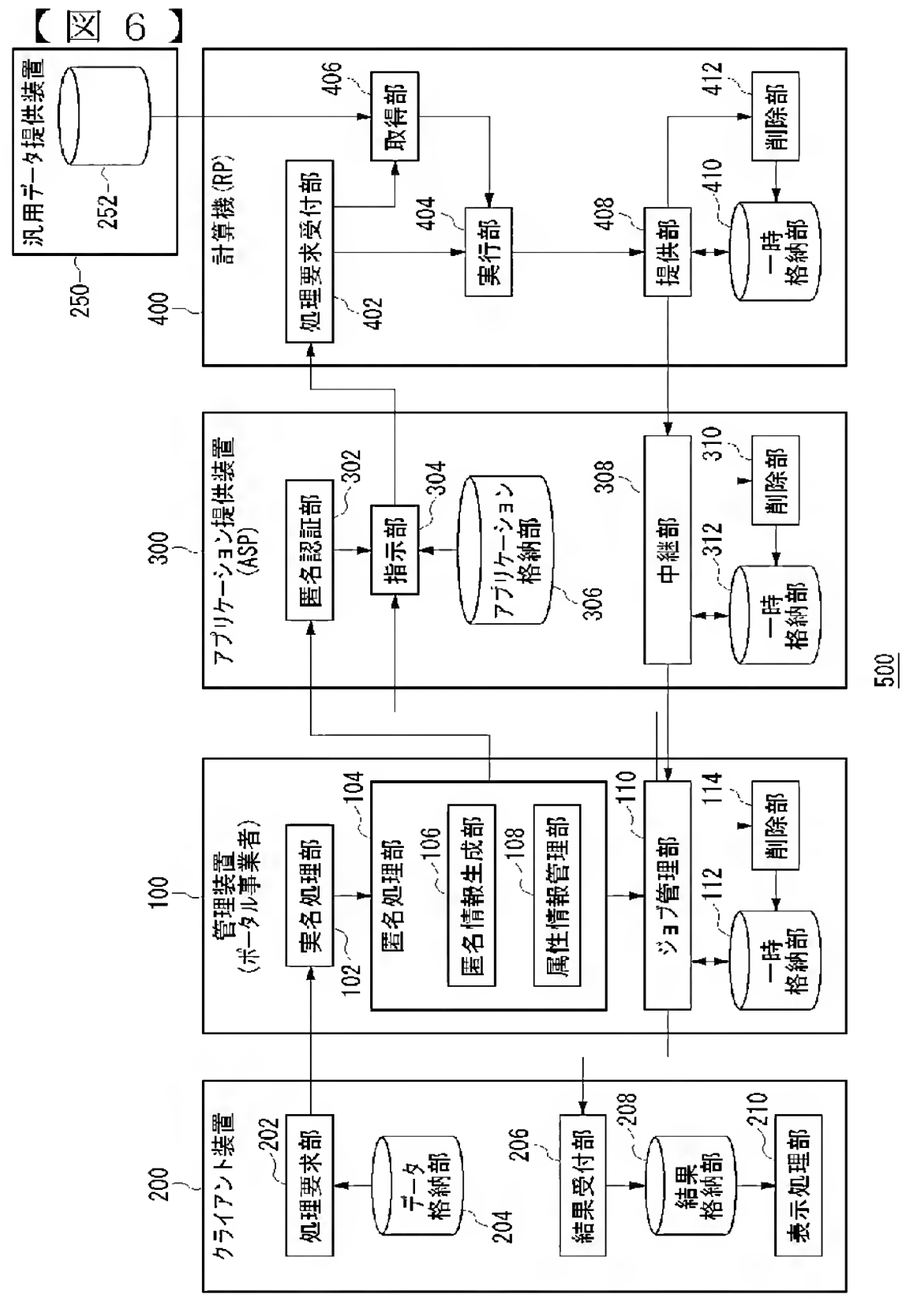
【図４】


年齢
性別
○○サイトの会員情報の
有無
職種
居住地
処理に必要な属性
(と判断したもの)
のみを回答する
100
管理装置(ポータル事業者)
ユーザ属性証明書
634
匿名属性証明書
636
ユーザまたはポータルサイト上に
匿名属性証明書保存
(属性証明書からの変換可能)
ユーザ
630
プロセス実行の要求
プロセス実行
条件の打診
S100
属性
問い合わせ
S102
属性回答
S104
ユーザ認証
リソース割り当て
プロセスの実行
グリッド環境のサーバ
データ
アプリケーション
632

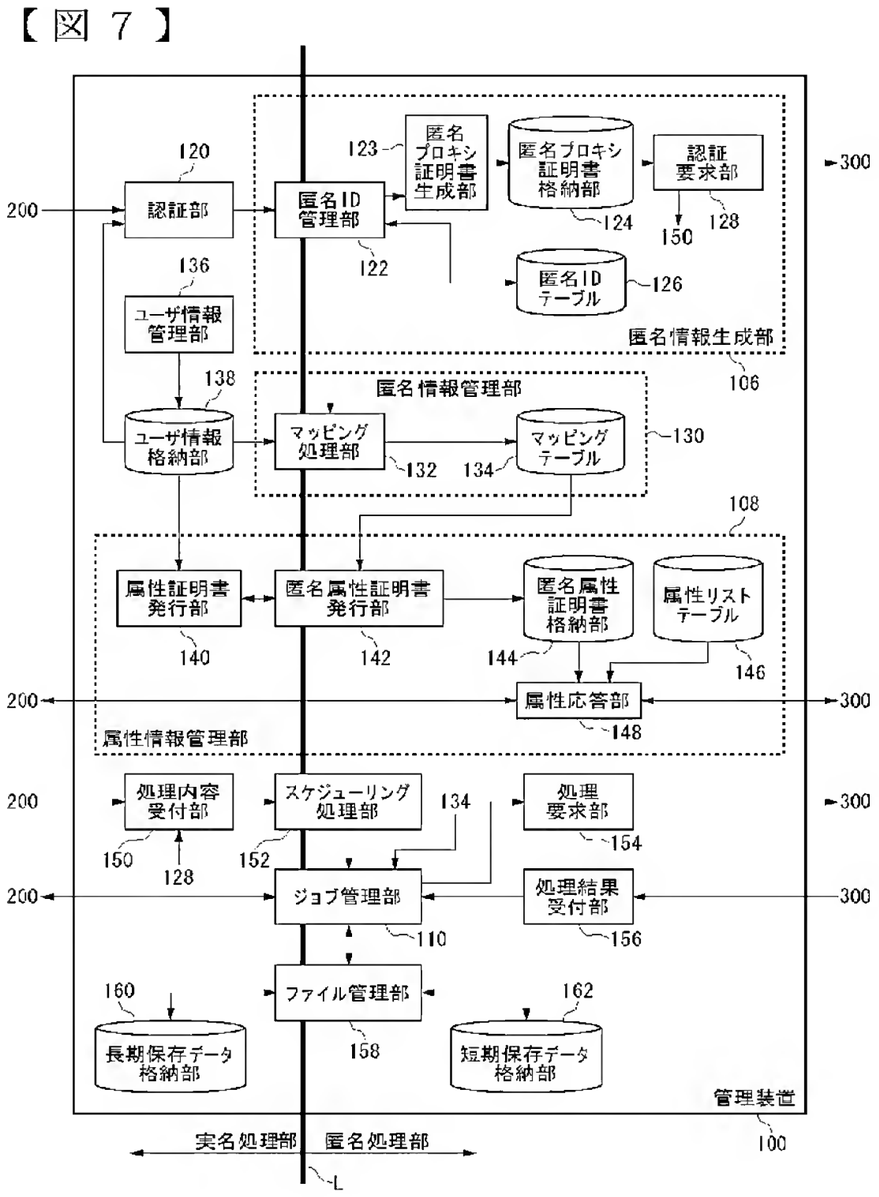
【図５】


管理装置(ポータル事業者)
100
実名処理部
102
ユーザ管理情報
匿名テーブル
ユーザ認証
実ユーザと匿名ユーザとのマッピング
長期保存データ(実名でアクセス可能)
94
匿名処理部
104
データ保存、管理
短期保存データ(匿名でアクセス可能)
96
匿名ユーザによるデータアクセス
データ転送
プロセス実行含むデータアクセス要求
ユーザ
データ
630
グリッド環境のサーバ
632
ユーザ認証
データI/O
データ
基本的に処理後データ消去

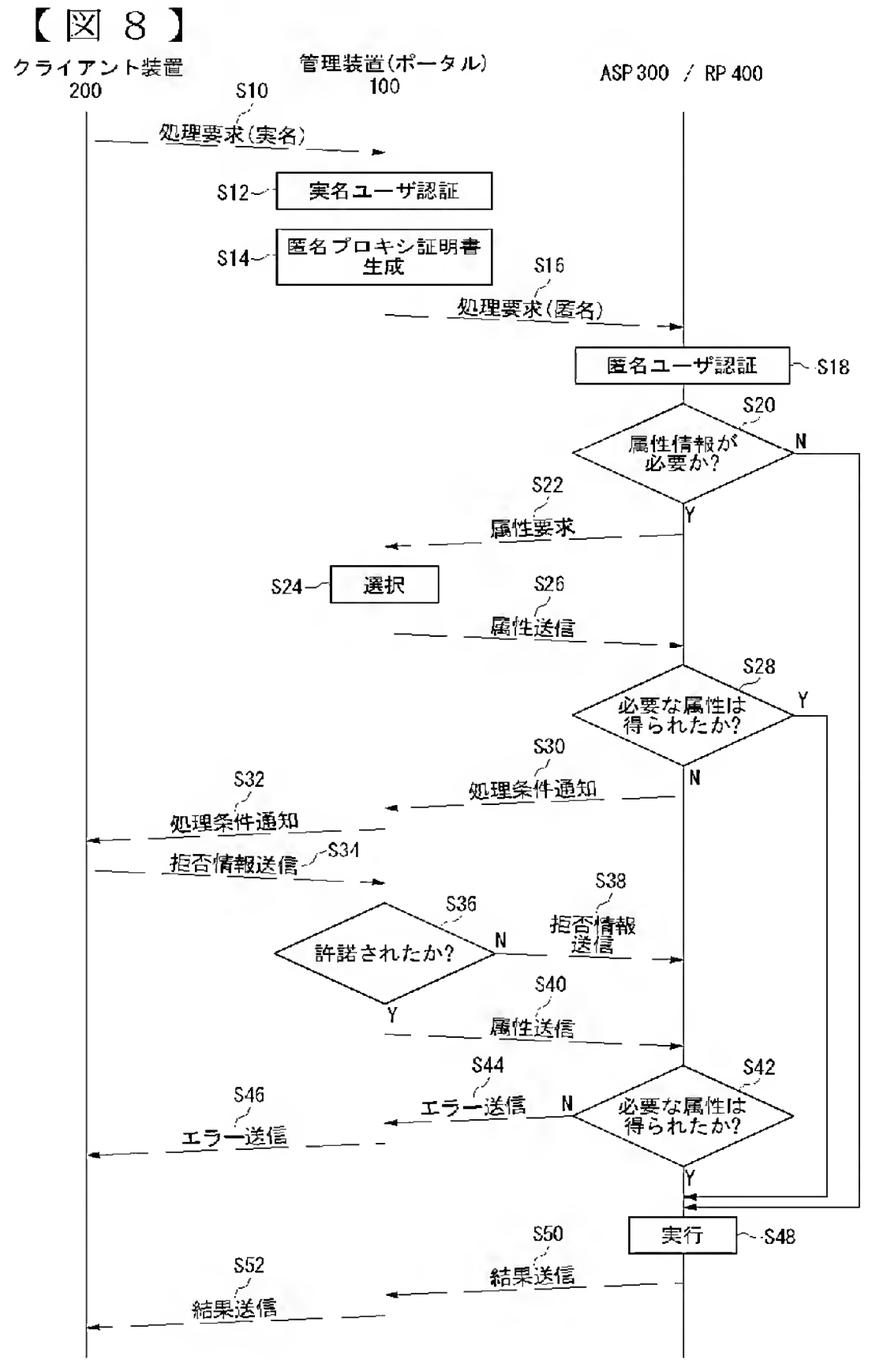
【図６】


汎用データ提供装置
252
250
計算機(RP)
400
処理要求受付部
402
取得部
406
実行部
404
提供部
408
一時格納部
410
削除部
412
アプリケーション提供装置(ASP)
300
匿名認証部
302
指示部
304
アプリケーション格納部
306
中継部
308
一時格納部
312
削除部
310
500
管理装置(ポータル事業者)
100
実名処理部
102
匿名処理部
104
匿名情報生成部
106
属性情報管理部
108
ジョブ管理部
110
一時格納部
112
削除部
114
クライアント装置
200
処理要求部
202
データ格納部
204
結果受付部
206
結果格納部
208
表示処理部
210

【図７】


300
200
認証部
120
匿名ID管理部
122
匿名プロキシ証明書生成部
123
匿名プロキシ証明書格納部
124
認証要求部
128
150
匿名IDテーブル
126
匿名情報生成部
106
ユーザ情報管理部
136
ユーザ情報格納部
138
匿名情報管理部
マッピング処理部
132
マッピングテーブル
134
130
108
属性証明書発行部
140
匿名属性証明書発行部
142
匿名属性証明書格納部
144
属性リストテーブル
146
属性応答部
148
属性情報管理部
処理内容受付部
150
128
スケジューリング処理部
152
134
処理要求部
154
ジョブ管理部
110
処理結果受付部
156
ファイル管理部
158
160
長期保存データ格納部
162
短期保存データ格納部
管理装置
100
実名処理部
匿名処理部
L

【図８】


クライアント装置
200
管理装置(ポータル)
100
ASP 300 / RP 400
S10
処理要求(実名)
S12
実名ユーザ認証
S14
匿名プロキシ証明書生成
S16
処理要求(匿名)
匿名ユーザ認証
S18
S20
属性情報が必要か?
N
Y
S22
属性要求
S24
選択
S26
属性送信
S28
必要な属性は得られたか?
Y
N
S30
処理条件通知
S32
処理条件通知
S34
拒否情報送信
S36
許諾されたか?
N
Y
S38
拒否情報送信
S40
属性送信
S44
エラー送信
N
S42
必要な属性は得られたか?
S46
エラー送信
Y
実行
S48
S50
結果送信
S52
結果送信

フロントページの続き

(72)発明者　伊藤　智
茨城県つくば市東１－１－１　独立行政法人産業技術総合研究所つくばセンター内
(72)発明者　高木　浩光
茨城県つくば市東１－１－１　独立行政法人産業技術総合研究所つくばセンター内
(72)発明者　森尻　智昭
東京都港区芝浦一丁目１番１号　東芝ソリューション株式会社内
(72)発明者　才所　敏明
東京都港区芝浦一丁目１番１号　東芝ソリューション株式会社内

Ｆターム(参考) 5B285 AA04 CA43 CB47 CB51 CB91
5J104 KA01 PA07

PAT-NO: JP02006301831A

DOCUMENT-IDENTIFIER: JP 2006301831 A

TITLE: MANAGEMENT DEVICE

PUBN-DATE: November 2, 2006

INVENTOR-INFORMATION:

NAME	**COUNTRY**
TANAKA, YOSHIO	N/A
SEKIGUCHI, TOMOTSUGU	N/A
ITO, SATOSHI	N/A
TAKAGI, HIROMITSU	N/A
MORIJIRI, TOMOAKI	N/A
SAISHIYO, TOSHIAKI	N/A

ASSIGNEE-INFORMATION:

NAME	**COUNTRY**
NATIONAL INSTITUTE OF ADVANCED INDUSTRIAL & TECHNOLOGY	N/A
TOSHIBA SOLUTIONS CORP	N/A

APPL-NO: JP2005120627

APPL-DATE: April 19, 2005

INT-CL-ISSUED:

TYPE	**IPC**	**DATE**	**IPC-OLD**
IPCP	G06F21/20	20060101	G06F021/20

IPFC G09C1/00 20060101 G09C001/00

ABSTRACT:

PROBLEM TO BE SOLVED: To provide a technique facilitating authentication processing in a grid environment and a technique attaining a secure grid environment.

SOLUTION: A grid system 600 is connected to a client device 200 through SSL and performs authentication based on a user's ID or password. When the authentication is successful, an authentication part 612 instructs generation of an anonymous proxy certificate to a proxy certificate generation part 616. The proxy certificate generation part 616 reads preliminarily registered anonymous user information from an anonymous information storage part 618, and generates an anonymous proxy certificate 620 based on the anonymous information. The management device 610 performs authentication processing to a computer 400 using the anonymous proxy certificate 620 to make the computer execute jobs. The computer 400 accepts the validity of the anonymous proxy certificate 620 by trusting the management device 610. By using the anonymous proxy certificate in this way, transfer of personal information of a user to the computer 400 can be prevented.